ボットネットの実態と対策

KDDI研究所
竹森敬祐

- ボットネットの実態調査
- ボット感染検知システム

実態：ボットネットとは

■ ボットネット

指令者

指令サーバ

ボット

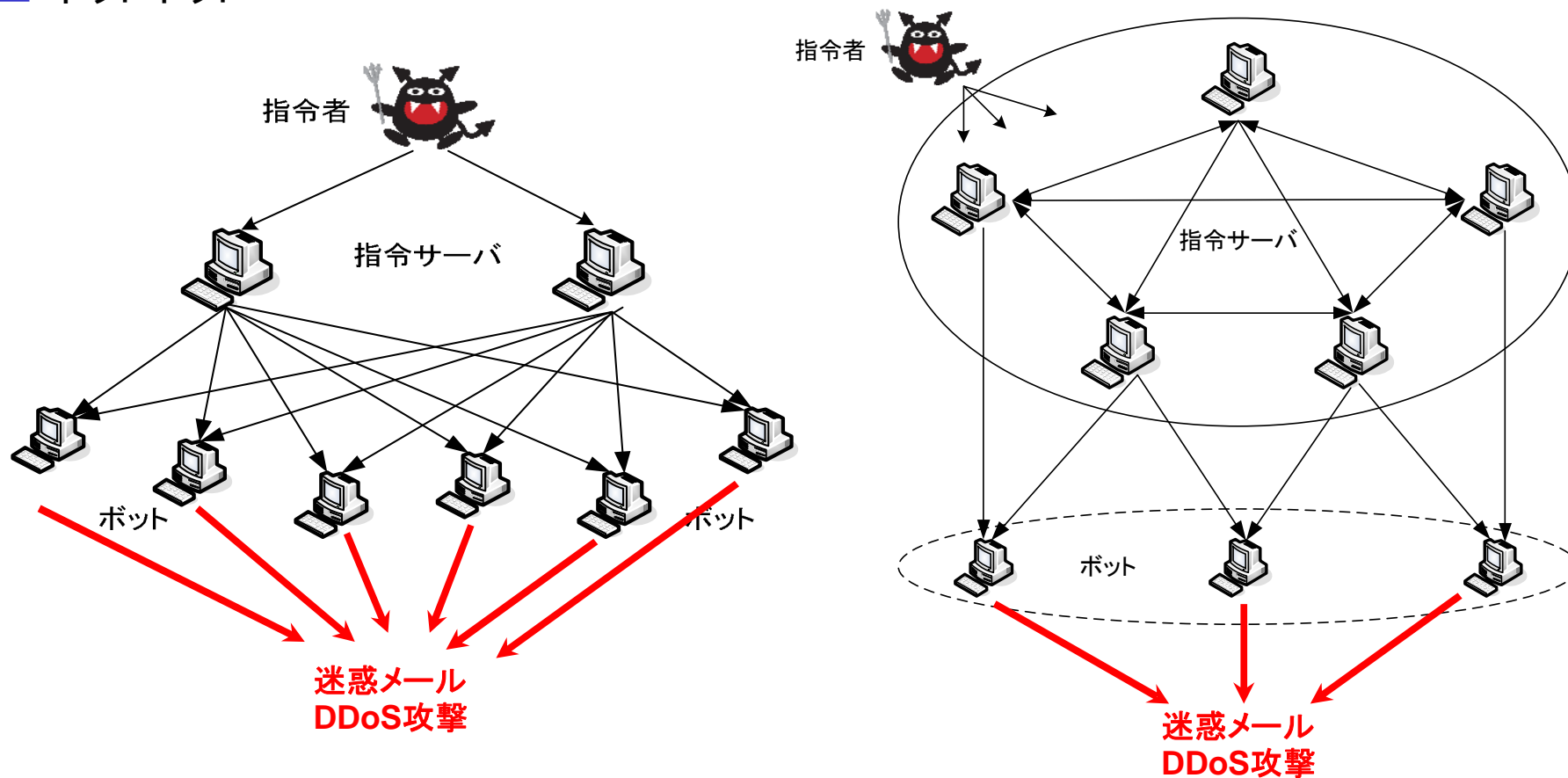
ボット

迷惑メール
DDoS攻撃

指令者

指令サーバ

ボット

迷惑メール
DDoS攻撃

■ 課題

◆ 指令者は、効率的かつ安定的なボットネットの運用とボットの確保に努めている。

実態：多重感染

■ 解説

- ◆ 初期コードが削除され、5つのexeコードが追加され、hostsが改竄された。
- ◆ AVで初期コード、2つのexeコード、hostsが検知され、**2つのexeコードが残っている。**

HoneyPot Management System - Windows Internet Explorer

http://192.168.1.101/main.php?sh=nepdet&time=2008-05-14%2021:21:

Content(s) of Zip file :

Filename	Filesize
firewall.exe	214528 bytes
fwxurpon.exe	26112 bytes
hosts	11359 bytes
logon.exe	69120 bytes
mdtaj.exe	23040 bytes
upqdrmv.exe	26112 bytes

5つのexeとhostsファイルを追加・変更

Packet Capture File :

Timestamp	Filename	Filesize	Download
2008-05-14 21:21:45	20080514-212145.pcap	250052 bytes	

Antivirus Scan Result : 3つのexeとhostsファイルを駆除

Timestamp	Filename	Result
2008-05-14 21:21:45	firewall.exe	W32/Virut.W
2008-05-14 21:21:45	hosts	TR/Qhost.AA
2008-05-14 21:21:45	logon.exe	TR/Crypt.NSPM.Gen
2008-05-14 21:21:45	/hpm/hp/hp0/df/2008/05/14/21/21/d629a8288c2b7ea394	W32/Virut.W

実態:トロイの木馬

- コードの生き残りの工夫
  - 追加・変更されたコードの一例を示す。
- 解説
  - これらの殆どが起動されることなく、HDDに保存されたままである。しかし、cmd.exeやexplorer.exe、bedaula.htm、などは, Windows PCが元々持つプログラムに感染しており、ユーザ操作の中で起動が期待されるトロイの木馬である。

トロイ

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 フォルダ

アドレス(D) 追加・変更されたコードセットの一例 移動

ファイルとフォルダのタスク
新しいフォルダを作成する
このフォルダを Web に公開する
このフォルダを共有する

その他
(1)20080503-155705(800r 単純スキャン
マイ ドキュメント
共有ドキュメント
マイ コンピュータ
マイ ネットワーク

agentsvr.exe
Microsoft Agent Server
Microsoft Corporation

NOTEPAD.EXE
Notepad
Microsoft Corporation

cmd.exe
Windows Command Processor
Microsoft Corporation

write.exe
Windows Write
Microsoft Corporation

explorer.exe
Windows Explorer
Microsoft Corporation

ftp.exe
File Transfer Program
Microsoft Corporation

badeula.htm
Firefox Document
4 KB

autoupdt.htm
Firefox Document
6 KB

ss3dfo.scr
スクリーン セーバー
700 KB

scrnsave.scr
スクリーン セーバー
19 KB

実態：多機能ボット

- プロセス通信モニタ
  - 著者らが開発したホスト型の通信プロセスモニタ[4]を用いて視覚化した様子を示す。
- 解説
  - exploere.exe，winamp.exe，winlogon.exeの3つのコードが起動して外部のPCと通信している。
  - 3つのコード は独立動作しており、様々なIP：Portに向かって通信している。

実態：hostsファイルの改ざん

- アンチウイルス（AV）の無効化
  - /WINDOWS/sytem32/drivers/etc/hostsファイルを改ざんしてAVの自動更新を阻止する。

hosts - メモ帳

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

```
127.0.0.1       localhost
127.0.0.1       www.symantec.com
127.0.0.1       securityresponse.symantec.com
127.0.0.1       downloads1.kaspersky-labs.com
127.0.0.1       downloads2.kaspersky-labs.com
127.0.0.1       downloads3.kaspersky-labs.com
127.0.0.1       downloads4.kaspersky-labs.com
127.0.0.1       downloads5.kaspersky-labs.com
127.0.0.1       www.kaspersky-labs.com
127.0.0.1       symantec.com
127.0.0.1       www.sophos.com
127.0.0.1       sophos.com
127.0.0.1       www.mcafee.com
127.0.0.1       mcafee.com
127.0.0.1       liveupdate.symantecliveupdate.com
127.0.0.1       www.viruslist.com
127.0.0.1       viruslist.com
127.0.0.1       viruslist.com
127.0.0.1       f-secure.com
127.0.0.1       www.f-secure.com
```

実態：多重感染(2)

■ 8つのコードセット
◆ 各コードに感染して10分後の、コードと設定の追加・変更・削除の様子をTripwireで確認。

■ 解説
◆ 複数のコードを取得して、多数のコードを書き込み、多数の設定を改ざんする。

セット	コード		設定の追加・変更・削除	
	追加	変更	レジストリ	hosts
1	4 (exe)	527(exe,htm,scr)	305	有(127型)
2	3 (exe)	422 (exe,scr)	311	有(255型)
3	107(exe)	106 (htm)	15	無
4	5 (exe)	0	3	有(255型)
5	6 (exe)	0	3	有(127型)
6	6 (dll,exe)	3 (ini,sys)	115	無
7	5 (exe)	0	4	有(127型)
8	4 (dll,exe)	1 (ini)	7	有(255型)

実態：未知のコードと攻撃パケット

■ アンチウイルス（AV）の検知率

- ◆ Bot感染後に変化した661種類のファイルに対して、AVの検知率を評価した。
- ◆ もしAVで5個以上のBotが検知された場合には、1個以上のBotを駆除できずに、PC内に潜んでいることになる。

検知率		1位		2位		3位		4位		5位	
総数=661		K-AV		Z-AV		N-AV		C-AV		T-AV	
Tripwire検知	既知	555件	84.0%	554件	83.8%	540件	81.7%	537件	81.2%	521件	78.8%
	未知	106件	16.0%	107件	16.2%	121件	18.3%	124件	18.8%	140件	21.2%

■ 侵入検知システム（IDS）によるOutboundパケット検知

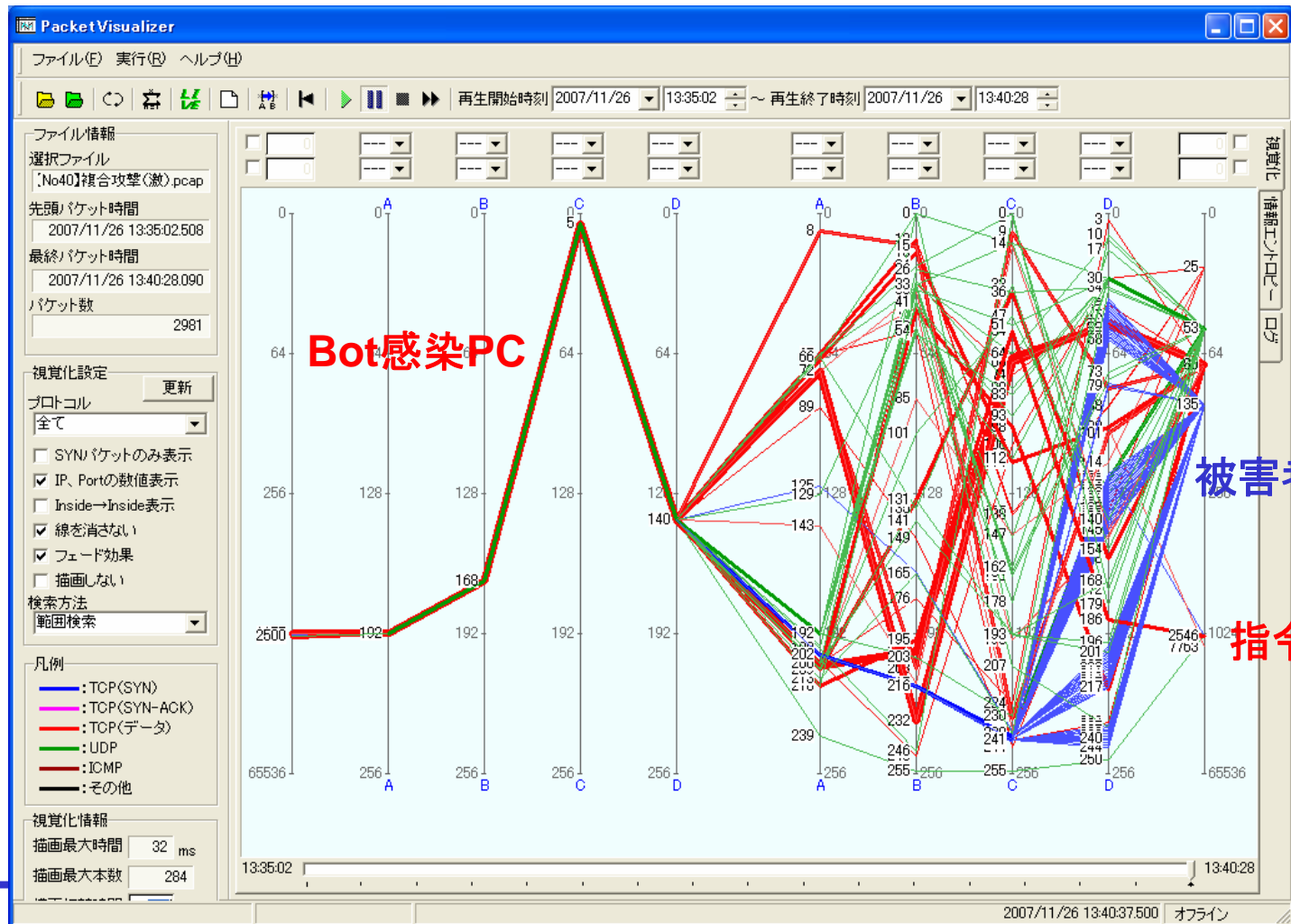
- ◆ 37種類のBotコードがOutboundパケットを発信した。このときのIDSの検知率を評価した。
- ◆ 感染後に、正しいプロトコルで通信を行うと、検知が難しい。

感染PCからのOutboundパケットのIDS検知

	I-IDS	P-IDS
検知数	26/37件	20/37件
検知率	70.3%	54.1%

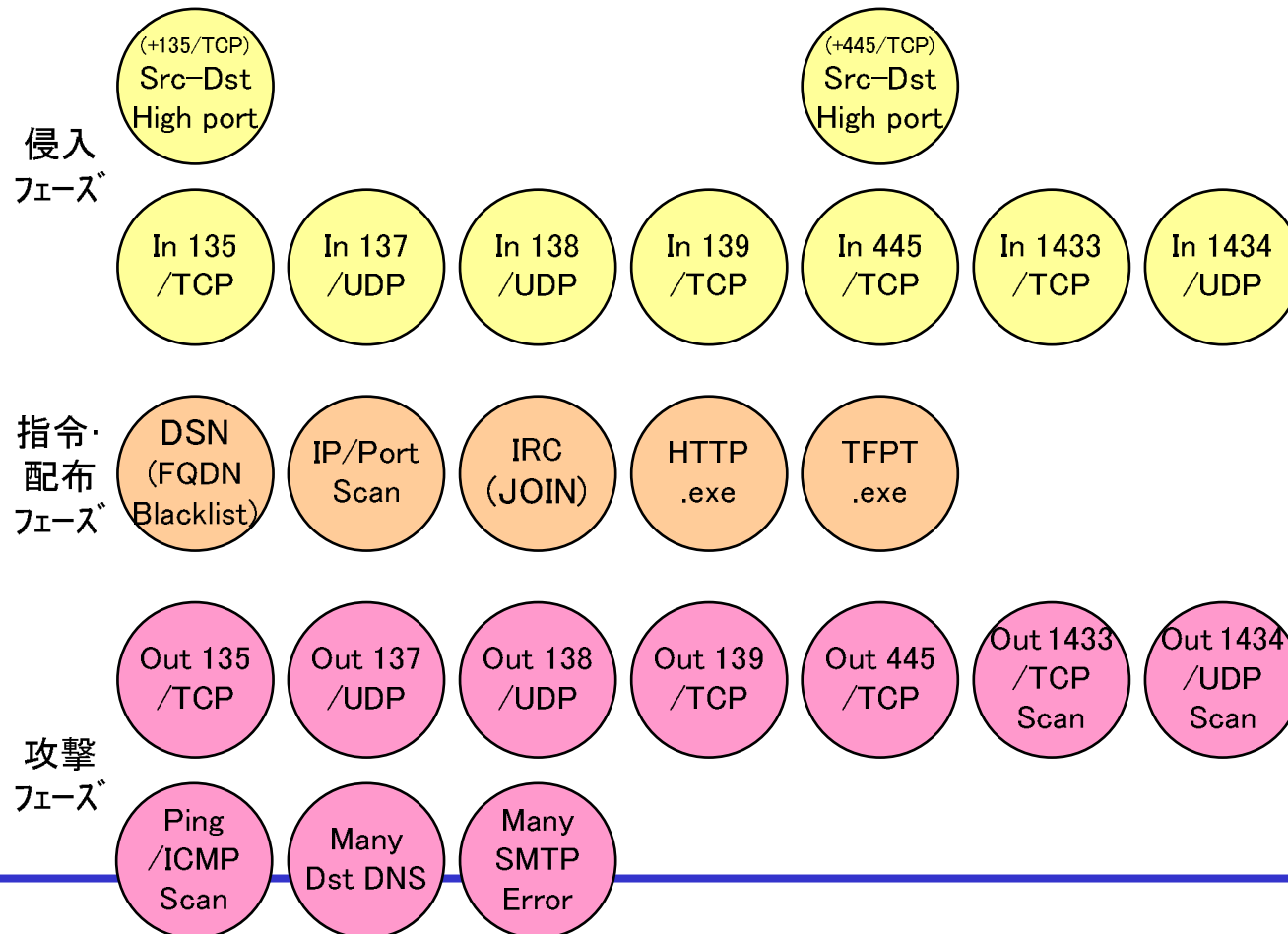
実態：Outbound通信

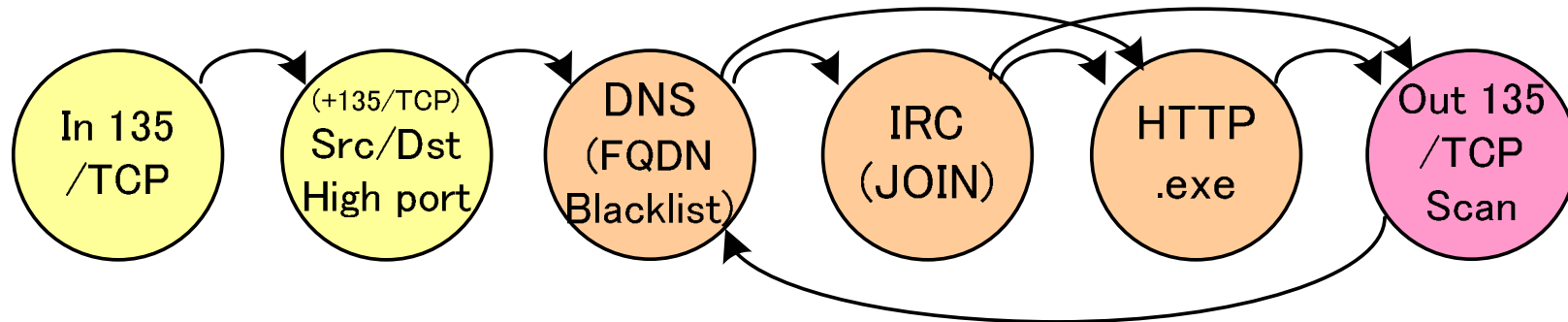
- ウイルス（Botと呼ぶ）の通信パターン
  - ◆ このBotの通信速度：0.05Mbps、9.0 pps
    - ⇒ 通信速度が遅いため感染の異変に気付かない。

KDDI R&D LABS

対策：ボットの通信要素

■ 通信要素の抽出

◆ ボットの通信データについてヒューリスティックな調査を繰り返し、ハニーポットへの侵入フェーズ、感染後の指令・配布フェーズ、外部への攻撃フェーズに含まれる、特徴的な通信要素について調査した。

侵入フェーズ	(+135/TCP) Src-Dst High port				(+445/TCP) Src-Dst High port		
	In 135 /TCP	In 137 /UDP	In 138 /UDP	In 139 /TCP	In 445 /TCP	In 1433 /TCP	In 1434 /UDP
指令・配布フェーズ	DSN (FQDN Blacklist)	IP/Port Scan	IRC (JOIN)	HTTP .exe	TFPT .exe		
攻撃フェーズ	Out 135 /TCP	Out 137 /UDP	Out 138 /UDP	Out 139 /TCP	Out 445 /TCP	Out 1433 /TCP Scan	Out 1434 /UDP Scan
	Ping /ICMP Scan	Many Dst DNS	Many SMTP Error				

対策：ボットの通信シナリオ

- 通信要素の組み合せである通信シナリオの抽出
  - 状態遷移モデル（a）の矢印を取り除いた通信要素の出現順序（b）を取り出して、これを通信シナリオとする。⇒厳密な検知
  - 通信シナリオの出現順序を無視した組み合わせにも着目する。⇒大よその検知

（a）通信要素の状態遷移モデル

In 135 /TCP	(+135/TCP) Src/Dst High Port	DNS (FQDN Blacklist)	IRC (JOIN)	HTTP . exe	Out135 /TCP

（b）通信要素の出現順位に注目した通信シナリオ

出現順序　or　出現組合せ

対策：Bot感染検知システムの実装

Bot Hunter – Windows Internet Explorer

Bot Hunter

詳細 | 統計(日) | 統計(月) | 手動 | システム設定

2009年 3月

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

・結果一覧

観測時刻	時間 [分]	Bot IP観測数	指令サーバ観測数	パケット数	回線速度	1次解析	2次解析
2009-03-13 00:00:45	15	7	6	18,373	12Kbps	完了	完了
2009-03-13 00:15:01	15	8	0	672	0Kbps	完了	完了
2009-03-13 00:30:00	15	10	6	185,651	107Kbps	完了	完了
2009-03-13 00:45:00	15	13	9	166,288	92Kbps	完了	完了
2009-03-13 01:00:00	14	5	1	75,633	43Kbps	完了	完了
2009-03-13 01:17:41	11	4	3	522	0Kbps	完了	完了
2009-03-13 01:30:05	15	9	3	400	1Kbps	完了	完了
2009-03-13 01:45:50	15	7	5	86,527	60Kbps	完了	完了

1次解析 | Bot→指令絞込み | 指令→Bot絞込み | 2次解析

観測時刻 2009-03-13 00:00:45 | 観測時間 [分] 15 | パケット数 18,373 | 注目NWグループ 全て | FQDN一括検索

・Bot検知情報: 観測数 7 件 | 注目NWアドレス抽出 | Botリストダウンロード

Start Time	Pcap	Bot IP	FQDN	指令サーバFQDN[IP]	BlackList	AV判定	IRC	HTTP *.exe
2009-03-13 00:00:45	1.7 MB	10.10.21.1	?	⊟ xx.ka3ek.com [67.43.226.242] alwayssam.com [67.215.1.206] zonetech.info [72.10.166.195]	176	有	⊟ NICK:14 #las6 #las6	⊟ /vot.exe /vot.exe /vss.exe /vss.exe
2009-03-13 00:12:16	3.5 KB	114.145.127.2	p4002-ipbf6202marunouchi.tokyo.ocn.ne.jp	0件	0		0件	0件
2009-03-13 00:09:26	5.8 KB	124.106.220.69	?	0件	0		0件	0件
2009-03-13 00:02:08	103.4 KB	124.86.165.111	p3111-ipbf1408marunouchi.tokyo.ocn.ne.jp	⊟ ? [10.10.21.1]	0		⊟ NICK:109	0件
2009-03-13 00:11:07	624Byte	60.169.3.49	?	0件	0		0件	0件
2009-03-13 00:02:15	4.2 KB	67.43.226.242	xx.ka3ek.com	⊟ ? [10.10.21.1]	0		⊟ NICK:8	0件

・指令サーバ情報: 観測数 6 件 | 注目NWアドレス抽出 | 指令サーバリストダウンロード

Start Time	Pcap	指令サーバIP	FQDN	Bot FQDN[IP]	BlackList	AV判定	IRC	HTTP *.exe
2009-03-13 00:00:45	1.7 MB	10.10.21.1	?	⊟ ? [124.86.165.111] xx.ka3ek.com [67.43.226.242]	0		⊟ NICK:117	0件
2009-03-13 00:03:47	131.8 KB	67.215.1.206	alwayssam.com	⊟ ? [10.10.21.1]	96	有	⊟ NICK:2	⊟ /vot.exe /vot.exe

インターネット | 100%

まとめ

■ 実態調査

- ◆ ボットは、自身のコードをアップデートすることで検知を逃れている。
  - ⇒ AVやIDSなどで多視点で対策を図る必要がある。
- ◆ 多重感染、トロイの木馬化、AVの無効化など、様々な影響が出る。
  - ⇒ 感染が確認された場合には、OSの再インストールを推奨する。

■ 対策研究

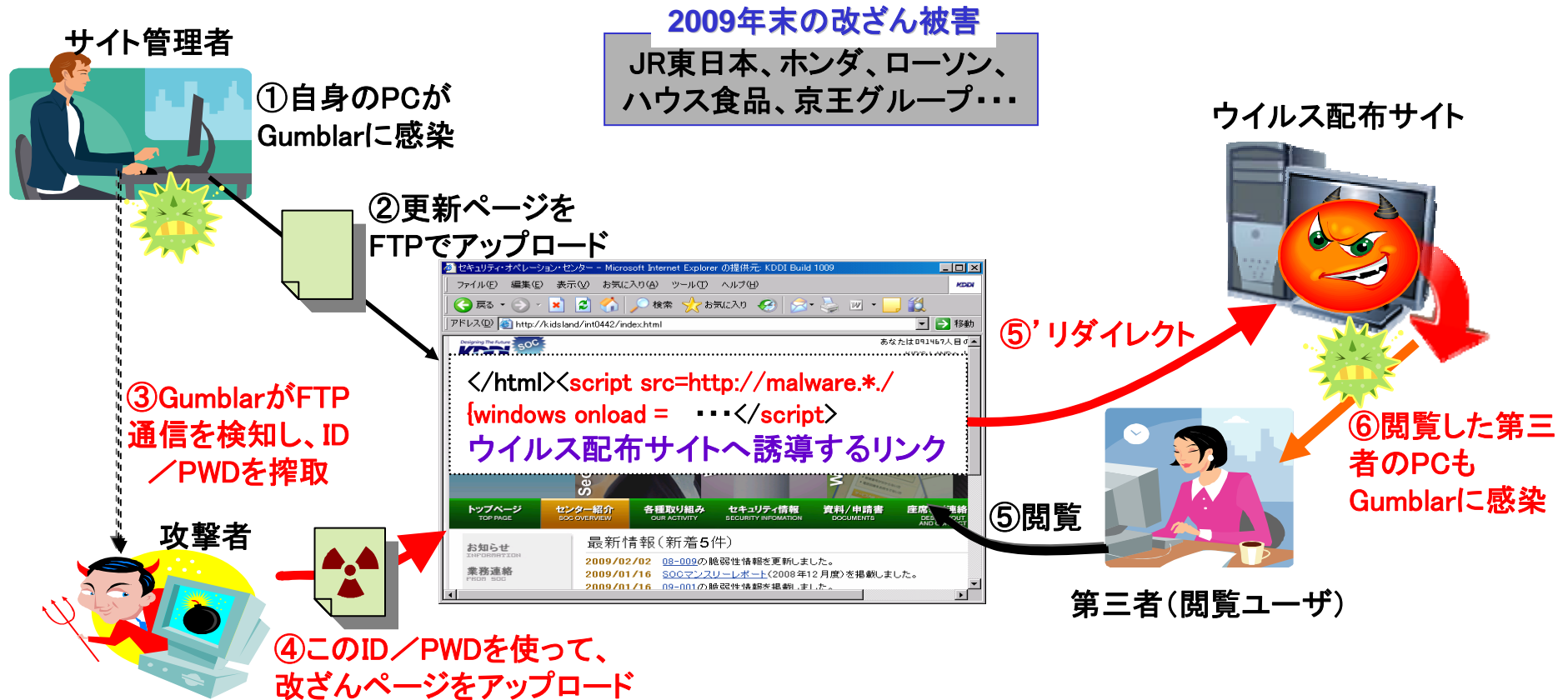
- ◆ 通信のシナリオに注目した感染検知システムを開発した。
  - ⇒ 通信の異常性に注目したアルゴリズムであり未知のボットを検知できる。

Web改ざん検知システム

KDDI研究所
竹森 敬祐

特徴

- Webページのダウンロードによるリモート監視
- 「更新」「改ざん」「障害」を区別してアラーム通知
- ウイルス配布型と悪性画像型の改ざんに対応
- Webページの構文解析による悪性箇所の指摘
- 簡単操作

最近の改ざん事情 ～ウイルス配布型のGumblar～

【Gumblarの改ざんパターン】

2009年12月以降） 改ざんチーム名と難読化スクリプトが埋め込まれる。

2009年10～12月）'<script src=' で始まり、'.php >' で終わるタグが埋め込まれる。

2009年5～10月） 「gumblar.cn」等の悪性サイトへのリンクが埋め込まれる。

Webサイト監視の課題とゴール

■ 課題

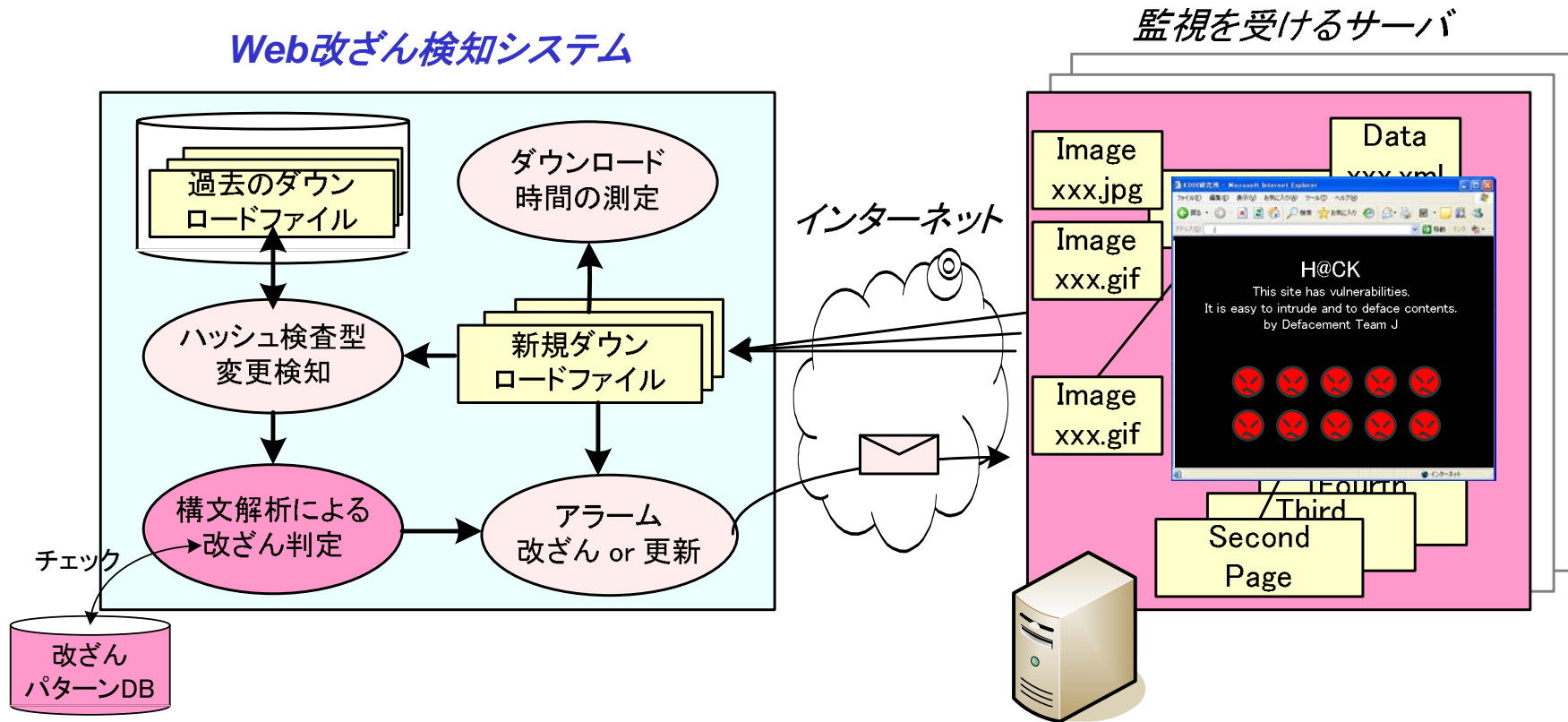
◆ 既存の監視システムでは、ページの変化に対してアラームを発信

■ ゴール

◆ ページの構文を解析して「更新」と「改ざん」を判定

KDDIのWeb改ざん検知システム

■ 機能構成

- ◆ リモートから複数のWebサーバを一括監視
- ◆ 改ざんパターンDBによる構文解析

【世界初】改ざんパターンDBを搭載

注目する特徴 ～ウイルス配布型改ざん～

■ ウイルス配布型の改ざん

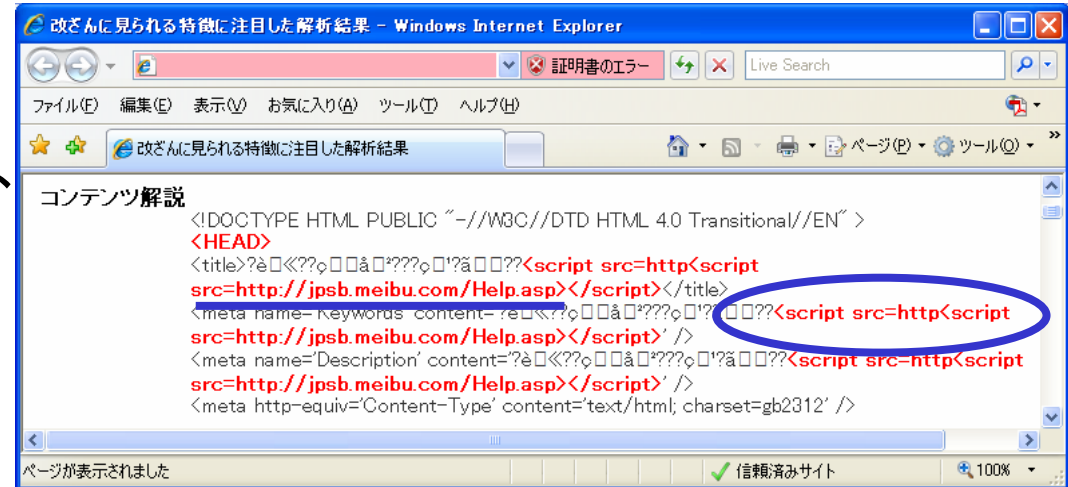
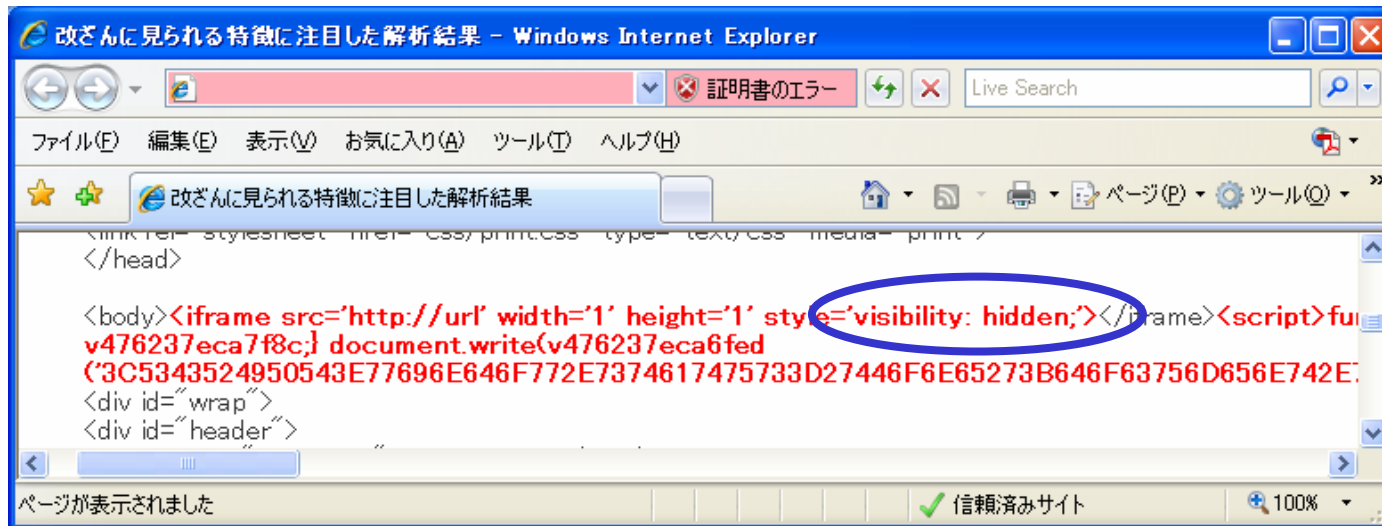
◆ 構文の崩れ

⇒ 機械的な改ざん文字の挿入で、HTMLタグの関係が崩れる。

◆ 悪性URLの挿入

⇒ ウイルス配布サイトへのリンクが追加される。

◆ 小さな挿入

⇒ 非表示リンクが埋め込まれる。

構文の崩れと悪性URLの挿入

非表示リンクの挿入

注目する特徴 ～悪性画像型改ざん～

■ 悪性画像型の改ざん

- ◆ 背景が黒い　<bgcolor=black>, <bgcolor=#00000000>
- ◆ 言語コードの変化　<charset>
- ◆ 悪性キーワード　hack, fuck, deface, ・・・

JPドメインWeb改竄速報
http://izumino.jp/Security/def_jp.html

悪性キーワードの登録画面
（KDDI-SOCによる登録）

差別化技術

既存のWeb変更検知システム

- サーバの内部から監視
  欠点1 ⇒ サーバ毎に監視システムをインストールするコスト
- 手動設定
  欠点2 ⇒ 監視対象ページを個々に登録する煩雑な運用
  欠点3 ⇒ 追加・削除されるたびに監視対象ページを再設定

KDDIのWeb改ざん検知システム

- 監視センタからリモート監視
  利点1 ⇒ 多数のWebサイト一括監視することでコストを抑制
- 自動設定
  利点2 ⇒ TOPページからリンクを辿りサイト内を網羅的に監視
  利点3 ⇒ ページ構成の変化を把握し24時間365日の全自動化

まとめ

■ 改ざんの種類

◆ 愉快犯による悪性画像型から、組織犯による感染型へ推移している。

◆ 一見すると改ざんと見抜けない。脆弱なブラウザが自動攻撃されてマルウェアに感染する。

■ 監視のサービス化

◆ 販売代理店：　ネットワールド　http://www.kaizankenchi.jp/

Android携帯電話のセキュリティ
～セキュアアプリ検証～

KDDI研究所
竹森　敬祐

Androidのリスク分析

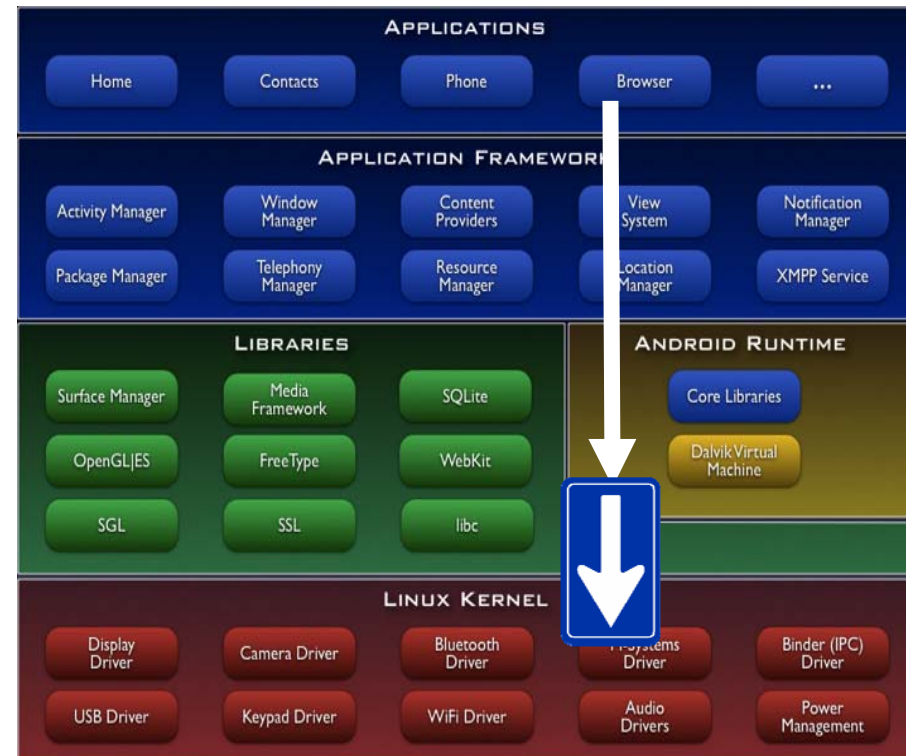
■ Android OS（Google社）の思想
- ◆ Android端末は、モバイル機能が付いたPCである。
- ◆ セキュリティはユーザ責任である。
- ◆ アプリケーションの開発と販売の自由化を図り、開発者とユーザを集める。

■ 今後の予測
- ◆ PCの利用経験のない世代まで、Android端末は普及する。
  - ⇒ PCで発生していたインシデントが、普及数に比例して発生する。
  - ⇒ 特に、ユーザの誤操作によるマルウェア感染が懸念される。

■ 課題
- ◆ KDDIとして、お客様に安心・安全にAndroid端末をご利用頂くための研究・開発が必要。

Androidの特徴

■ セキュリティ対策と脆弱性
◆ LinuxにDalvik仮想マシンを実装し、アプリをサンドボックス上で実行する。
◆ デフォルトオープンな通信Portは無い。アプリのインストールにはユーザ承認が必要。
⇒ Windows XPのような自動感染型ウイルス・ワームの影響は殆どない。
★ アプリ・パーミッションを承認することで、ユーザがサンドボックスに穴を開けることができる。
⇒マルウェア感染と、それを踏み台にしたインシデントが問題となる。

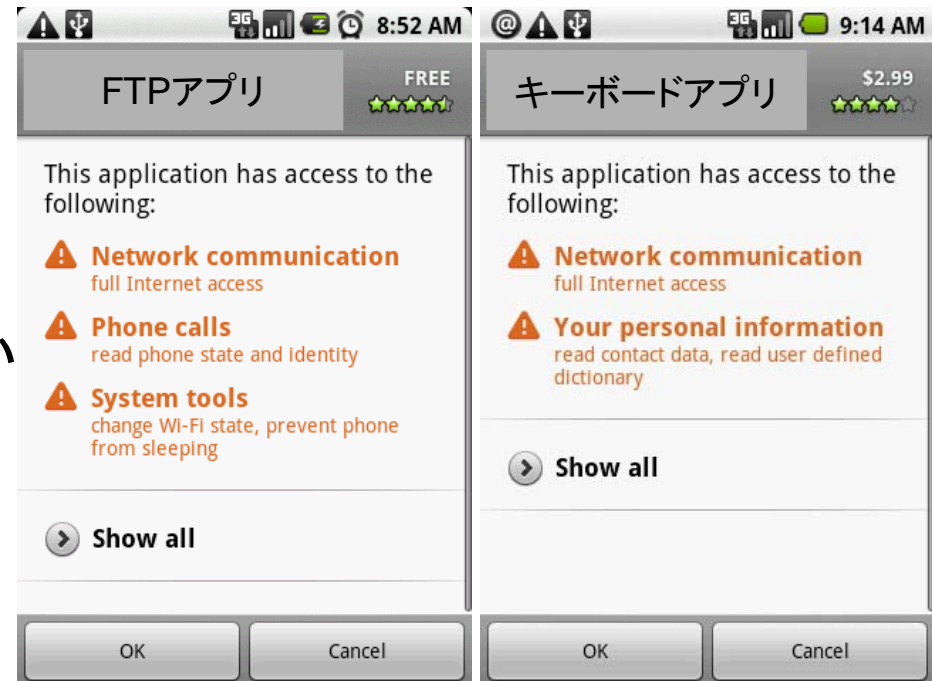
マーケットプレイスから入手したマルウェアに感染する事故が多発する?!

パーミッションによる承認

■ Dalvik VMの特徴

◆ ユーザは、アプリのパーミッション(潜在脅威)を閲覧してインストールを判断する。

■ パーミッションフレームワークの功罪

功 ユーザ承認で、個人情報や各種機能を利用する便利なアプリを実装できる。

罪 パーミッションの潜在脅威を見抜けないユーザは、マルウェアに感染する。

■ 問題点

◆ 機能単位の利用申請であり、悪意の有無とは直接関連しない。

◆ そもそもパーミッションを気にするユーザは少ない…。

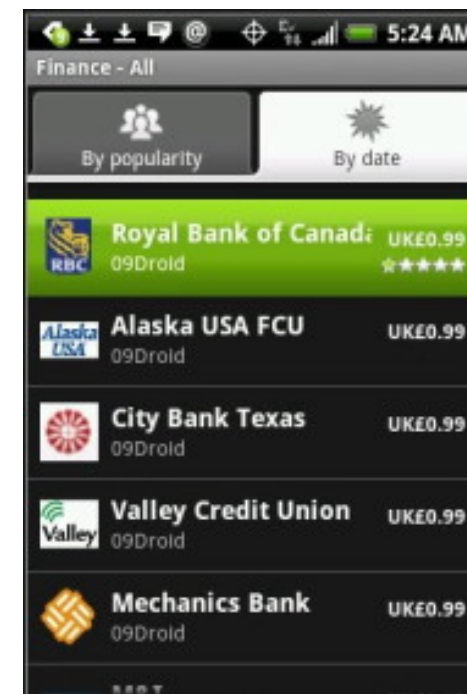
⇒ Android標準のパーミッション承認の機構では、不十分なのでは?!

25

実態：フィッシングアプリの一例

■ オンラインバンキング

◆ Droid09と呼ばれる匿名の開発者がリリースしたオンラインバンキングアプリがフィッシングアプリであったとの報告がある。

http://www.itmedia.co.jp/enterprise/articles/1001/12/news018.html
http://journal.mycom.co.jp/news/2010/01/14/019/index.html

■ キーモニタ・パーミッション

◆ android.permission.READ_INPUT_STATE

入力や操作の記録。別のアプリケーションへの入力（パスワードなど）でもキー入力を監視することをアプリケーションに許可します。通常のアプリケーションではまったく必要ありません。

■ 問題点

◆ 開発者の署名は未承認証明書で付すことができ、匿名性がある。

◆ オンラインバンキングのフィッシングアプリは簡単に作成できる。また、パーミッション（READ_INPUT_STATE）で、他のアプリへの入力もキーロギングできる。

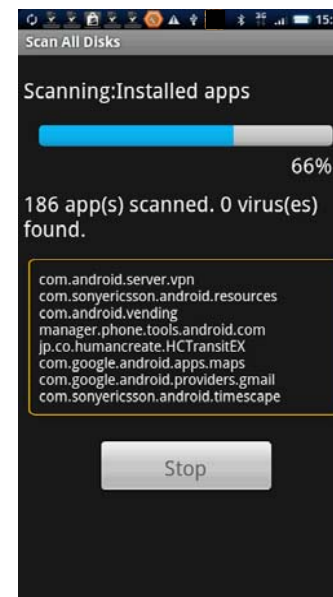
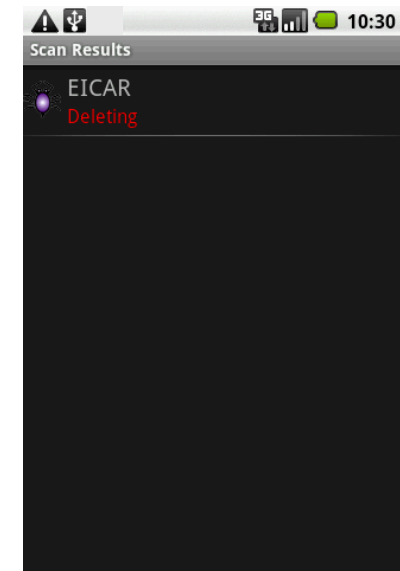
実態：スパイウェアの一例

■ 表面上の機能

- ◆ 某ウイルス対策アプリは、インストールアプリをスキャンしてウイルスを検知する。
- ◆ 本物のウイルスは一つも検知できない。

■ 31個のパーミッション
◆INTERNET、DELETE_PACKAGES、RESTART_PACKAGES、READ_PHONE_STATE、RECEIVE_SMS、READ_CONTACTS、WRITE_CONTACTS、CALL_PHONE、READ_SMS、WRITE_SMS、SEND_SMS、GET_TASKS、RECEIVE_BOOT_COMPLETED、INSTALL_PACKAGES、ACCESS_NETWORK_STATE、WRITE_APN_SETTINGS、PROCESS_OUTGOING_CALLS、INSTALL_SHORTCUT、LOCATION、ACCESS_FINE_LOCATION、ACCESS_LOCATION_EXTRA_COMMANDS、ACCESS_MOCK_LOCATION、ACCESS_COARSE_LOCATION、ACCESS_COARSE_UPDATES、CALL_PRIVILEGED、MODIFY_PHONE_STATE、GOOGLE_AUTH.mail、WAKE_LOCK、WRITE_EXTERNAL_STORAGE、USE_CREDENTIALS、VIBRATE

パーミッション承認

スキャンの様子

本物のウイルスを非検知

■ 問題点

- ◆ アプリの挙動をモニタしたところ、端末ID（IMEI）、契約 ID（IMSI）がアプリ作成者のサーバに送信された。

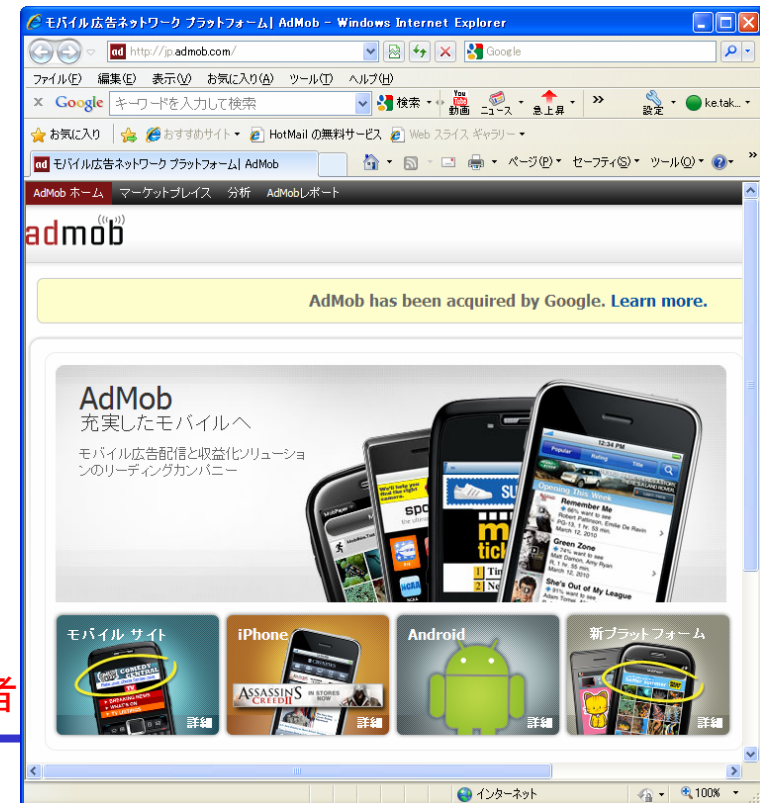
⇒ PCで起きていたトロイの木馬と同じことが発生している。

実態：アドウェアの一例

■ 無料アプリの収入源
- ◆ アプリに広告を掲載し、ユーザのクリックで開発者に報酬が入る。

■ 仕組み
- ◆ 国コード、緯度・経度を取得し、適切な言語で広告を表示する。
- ◆ TEL番号、Android ID、IMEI、IMSI 、広告先を識別する。

■ 問題
- ◆ 広告事業者は、情報の利用目的をユーザに知らせることなく、自動的に収集している。

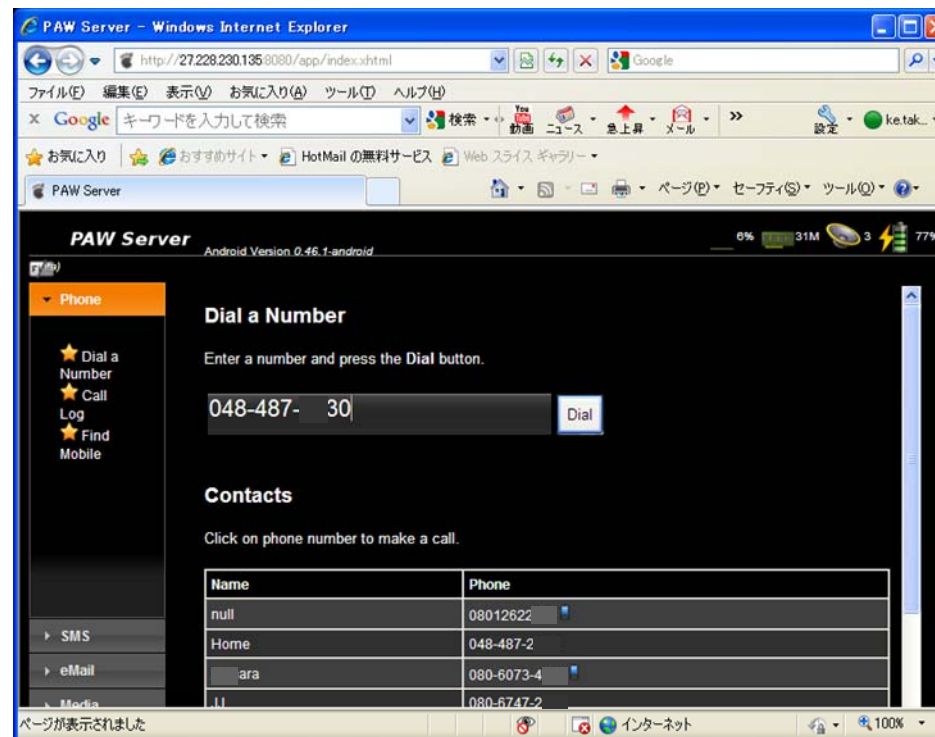
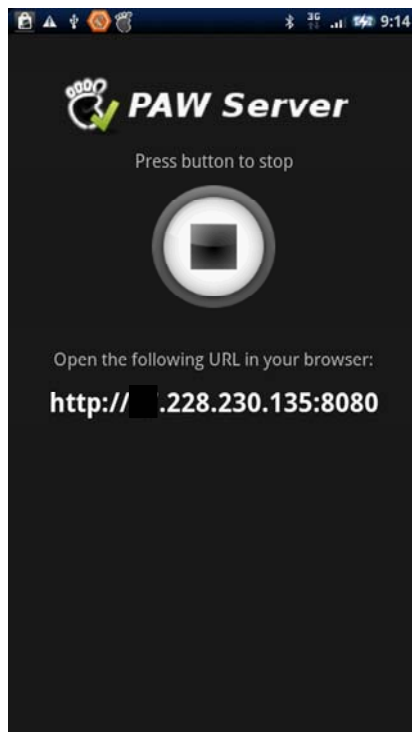
（パーミッションによる承認で、情報収集の可能性はユーザに確認済み。）

広告配信事業者

実態：リモート制御アプリの一例

■ リモート制御アプリ

◆ Android端末の操作を、リモートPCからプッシュ型で制御する。

注）下記は正常なアプリです。

グローバルIPを持つAndroid端末をリモート制御してTEL／メールさせるアプリ

■ 懸念

◆ 踏み台アプリによる、Android端末のボットネット化への悪用が可能である。

KDDIの取り組み：セキュアアプリ検証

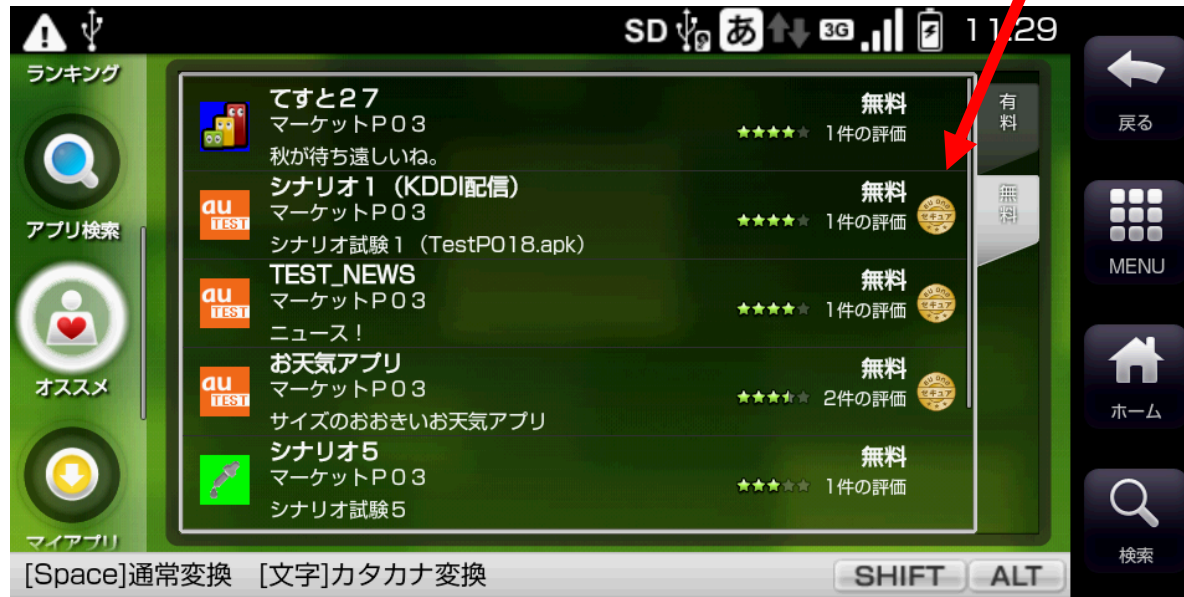
■ 感染源の分析

◆ 多くのユーザは、Marketプレイスを通じて、アプリを入手する。

⇒ Marketプレイスに安全なアプリしか無ければ、マルウェア感染を未然に防げる。

⇒ 難解なAndroidパーミッションの解読を、お客様に代わってKDDIが検証すべき。

■ ユーザ向けの安全なMarketサービス

◆ au one Marketセキュアアプリ検証を受けたアプリに、セキュアマークを付与している。

KDDIの取り組み：アプリ開発ガイドライン

■ アプリ開発者への啓蒙活動

◆ au one Marketセキュアアプリ検証で確認するポイントを明確にすることで、安全なアプリ開発を促している。

au one Marketセキュアアプリの検証では、以下の点に関する確認を実施しています。

1. 利用を宣言した機能（セキュリティー権限）の確認。
2. KDDIが提供しているAndroidアプリ配信サーバから配信していること。
3. KDDIから出荷されるAndroid端末の標準設定で利用できない機能の有無の確認。
4. 顧客情報を漏洩する動作、もしくは、漏洩する恐れのある動作の有無。
5. 不必要な大量通信の有無、もしくは、外部への不正アクセス機能の有無。

◆ 特に、重要な情報を外部へ送信する場合には、アプリケーションのストーリの中で、ユーザ承認を求める許諾画面を設けるように指導している。

（Androidのパーミッションフレームワークだけでは、不親切と考えている。）

KDDIの取り組み：ユーザへの啓蒙活動

■ 利用規約を通じた啓蒙活動

◆ Market運用者は、ユーザ責任でアプリのDL・インストール・利用について注意喚起している。

◆ 通信事業者は、さらに踏み込んで端末の取扱説明書を通じて、Market利用の危険性と自己責任に関する啓蒙活動に努めている。

Android Marketの免責

au one Marketの免責

IS01取扱説明書

免責事項について

◎地震・雷・風水害などの天災および当社の責任以外の火災、第三者による行為、その他の事故、お客様の故意または過失・誤用・その他異常な条件下での使用により生じた損害に関して、当社は一切責任を負いません。

◎本製品の使用または使用不能から生ずる附随的な損害（記録内容の変化・消失、事業利益の損失、事業の中断など）に関して、当社は一切責任を負いません。大切な電話番号などは控えておかれることをおすすめします。

◎本書と「取扱説明書詳細版」の記載内容を守らないことにより生じた損害に関して、当社は一切責任を負いません。

◎当社が関与しない接続機器、ソフトウェアとの組み合わせによる誤動作などから生じた損害に関して、当社は一切責任を負いません。

◎本製品の故障・修理・その他取り扱いによって、撮影した画像データやダウンロードされたデータなどが変化または消失することがありますが、これらのデータの修復により生じた損害・逸失利益に関して、当社は一切責任を負いません。

◎大切なデータはコンピュータのハードディスクなどに保存しておくことをおすすめします。万一、登録された情報内容が変化・消失してしまうことがあっても、故障や障がいの原因にかかわらず当社としては責任を負いかねますのであらかじめご了承ください。

Androidマーケットについて

◎アプリケーションのインストールは安全であることを確認のうえ、自己責任において実施してください。ウィルスへの感染や各種データの破壊などが発生する場合があります。

◎万一、お客様がインストールを行ったアプリケーションなどにより各種動作不良が生じた場合、当社では責任を負いかねます。

◎お客様がインストールを行ったアプリケーションなどにより、自己または第三者への不利益が生じた場合、当社では責任を負いかねます。